wherein the user is configured to decrypt a message based on an access policy using the secret key of attribute local trust of user u' issued by user u (SK_(LT, u, u')).

**93**. An apparatus according to claim **87**, wherein a user of the one or more users maintains a public key for user u (PK_u), wherein the public key (PK_u) comprises a user identification and a key to verify an access attribute.

**94**. An apparatus according to claim **87**, wherein a user of the one or more users maintains a secret key for user u (SK_u), wherein the secret key (SK_u) comprises decryption information configured to access the personalized decryption secret key.

**95**. An apparatus comprising:

at least one processor; and

at least one memory comprising computer program code, the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to at least:

receive a public encryption key and a personalized decryption secret key from a trusted server; and

encrypt a message configured to be broadcast to a plurality of users, the message being encrypted based on an access policy and the public encryption key.

**96**. An apparatus according to claim **95**, wherein the access policy defines access based on a trust level of at least one of general trust levels.

**97**. An apparatus according to claim **95**, wherein the message configured to be broadcast to the plurality of users is configured to be decrypted using one or more personalized decryption secret keys issued by the trusted server to the plurality of users in an instance in which a user of the plurality of users satisfy the access policy.

**98**. An apparatus according to claim **95**, wherein the public encryption key comprises a public key of attribute general trust (PK_GT) and the personalized decryption secret key comprises a secret key of attribute general trust of user u (SK_(GT, u)).

**99**. An apparatus according to claim **95**, wherein a user of the plurality of users maintains a public key for user u (PK_u), wherein the public key (PK_u) comprises a user identification and a key to verify an access attribute.

**100**. An apparatus according to claim **95**, wherein a user of the plurality of users maintains a secret key for user u (SK_u), wherein the secret key (SK_u) comprises decryption information configured to access the personalized decryption secret key.

**101**. An apparatus according to claim **95**, wherein the at least one memory comprising the computer program code is further configured to, with the at least one processor, cause the apparatus to:

receive a request for a key from one or more users;

generate a public encryption key and a personalized decryption secret key based on a local trust level for decryption of the one or more users; and

cause the personalized decryption secret key to be issued to one or more users in an instance in which the one or more users satisfy the local trust level for decryption.

* * * * *